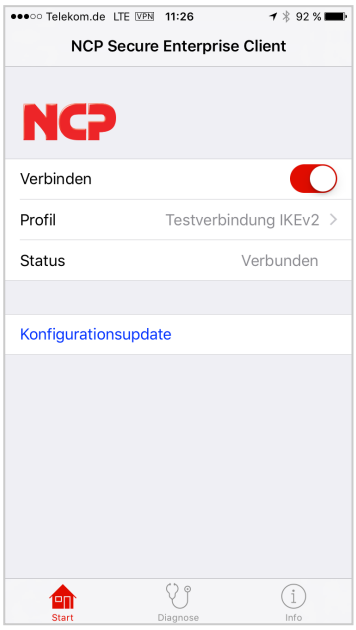
Datenblatt

NCP Secure Enterprise iOS Client

Zentral administrierbarer VPN Client für Apple iOS

- Zentrale Konfiguration und Zertifikats-Rollout via NCP Secure Enterprise Management
- NCP Load Balancing-Unterstützung
- Fallback IPsec / HTTPS (VPN Path Finder Technology)
- iOS Schlüsselbund-Unterstützung
- FIPS inside
- Starke Authentisierung, Touch ID-Unterstützung
- VPN On Demand



Universalität und Kommunikation

Der NCP Secure Enterprise iOS Client ermöglicht eine hochsichere VPN-Verbindung zu zentralen Datennetzen von Firmen und Organisationen. Der Zugriff ist auf mehrere unterschiedliche Daten-Netze mit jeweils eigenem VPN-Profil möglich. VPN On Demand ermöglicht den automatischen Aufbau des VPN-Tunnels und die ausschließliche Kommunikation darüber.

Die NCP VPN Path Finder Technology ermöglicht Remote Access auch hinter Firewalls bzw. Proxies, deren Einstellung VPN-Datenverbindungen grundsätzlich verhindert.

Sicherheit

Die starke Authentisierung des NCP Secure Enterprise iOS Client bietet einen umfassenden Schutz vor dem Fernzugriff unberechtigter Dritter. Unterstützt werden hierfür Zertifikate die in einem, für den NCP Secure Enterprise iOS Client, exklusiv genutzten Bereich des iOS-Schlüsselbundes abgelegt sind. Darüber hinaus kann der Aufbau einer VPN-Verbindung durch Authentifizierung via Fingerabdrucksensor (Touch ID) gesichert werden. Darüber hinaus kann der Aufbau einer VPN-Verbindung durch Authentifizierung via Fingerabdrucksensor (Touch ID) gesichert werden. Das Kryptografiemodul ist nach FIPS 140-2 gemäß Implementation Guidance section G.5 guidelines zertifiziert (Zertifikat #1747).

Wirtschaftlichkeit

Der NCP Secure Enterprise iOS Client bietet dem Anwender einfache Bedienung über seine grafische Benutzeroberfläche. Sie informiert über Verbindungsstatus, genutzte Zertifikate, sowie Netzwerkumgebung und bietet den Export von Log-Informationen. Dies ermöglicht niedrige Betriebskosten durch geringen Schulungsaufwand, weniger Dokumentation für den Anwender und schnelle Hilfe im Support-Fall.

Zentrales Management

Der NCP Secure Enterprise iOS Client ist für die zentrale Administration mit dem NCP Secure Enterprise Management (SEM) optimiert. Dadurch lassen sich Benutzerkonfigurationen und Zertifikats-Updates zentral verwalten. Zur Inbetriebnahme erhält der Client eine Minimalkonfiguration, um anschließend vom SEM seine individuelle Konfiguration und ggf. Zertifikate zu erhalten. Der Anwender ist nicht in der Lage, die zugewiesene Konfiguration einzusehen.

Voraussetzungen	iOS 11.x und höher; NCP Secure Enterprise VPN Server 11.0; NCP Secure Enterprise Management Server 4.05
Zentrales Management	Verteilung der VPN-Konfiguration und -Zertifikate über das NCP Secure Enterprise Management
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-konform; Event log; Kommunikation nur im Tunnel oder Split Tunneling; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Verschlüsselung (Encryption)	*Symmetrische Verfahren:* AES-CBC 128, 192, 256 Bit; AES-CTR 128, 192, 256 Bit; AES-GCM 128, 256 Bit (nur IKEv2); Blowfish 128, 448 Bit; Triple-DES 112, 168 Bit; SEED *Dynamische Verfahren für den Schlüsselaustausch:* RSA bis 4096 Bit; ECDSA bis 521 Bit, Seamless Rekeying (PFS); Hash Algorithmen: SHA, SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1, 2, 5, 14-21, 25-30
FIPS Inside	Der NCP Secure Enterprise iOS Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 gemäß Implementation Guidance section G.5 guidelines zertifiziert (Zertifikat #1747). Die FIPS Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden: ▪ DH-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit) ▪ Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit ▪ Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES
Schlüsselaustauschverfahren	IKEv1 (Aggressive und Main Mode Pre-shared key, RSA, XAUTH IKEv2 Pre-shared key, RSA, EAP-MS CHAPv2, EAP-MD5, EAP-TLS, EAP-PAP, Signature Authentication (RFC 7427), IKEv2 Fragmentation (RFC 7383)
Benutzer-Authentisierung	XAUTH bzw. EAP mit optionaler Eingabe des Benutzernamens und Passwortes vor dem manuellen VPN-Tunnelaufbau; Benutzerzertifikat im iOS Schlüsselbund; Touch ID zur Benutzerauthentisierung vor dem manuellen Aufbau des VPN-Tunnels
VPN Path Finder	NCP VPN Path Finder Technology, Fallback IPsec / HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist

IP Adress-Zuweisung	DHCP; IKE Config Mode (IKEv1); Config Payload (IKEv2)
Line Management	DPD mit konfigurierbarem Zeitintervall; Timeout; VPN On Demand für den automatischen Aufbau des VPN-Tunnels und die ausschließliche Kommunikation darüber
Datenkompression	Deflate
Weitere Features	UDP-Encapsulation;
Internet-Society RFCs und Drafts	RFC 4301 (IPsec), RFC 4303 ESP, RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IKEv1, RFC 3526, ISAKMP, RFC 7296 (IKEv2), RFC 4555 (MOBIKE), RFC 5685 (Redirect), RFC 7383 (Fragmentation), RFC 7427 , 3279 Section 2.2.3, 3447 Section 8 (Signature Authentication), RFC 5903, 6954, 6989, 4754 (ECC), RFC 2451, 3686 (AES with ESP), 5930 (AES-CTR), 4106 (AES-GCM), 5282, 6379 (Suite B), RFC 3447 Section 8 (Padding)
Client GUI Intuitive, grafische Benutzeroberfläche	Deutsch, Englisch; Konfigurations-Update; Profilauswahl; Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files; Fehlerdiagnose-Export; Netzwerkinformationen, 3D Touch
Bezugsquelle	NCP Secure Enterprise iOS Client kostenlos im App Store von Apple herunterladen. Kontaktieren Sie uns unter ios-client@ncp-e.com zum Testen der Software.

FIPS 140-2 Inside

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg
Germany

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com